6 Bảo mật và chuẩn hoá

Mục tiêu của chương:

Khi thông tin được trao đổi qua mạng, vấn đề an toàn và bảo mật cần được đảm bảo vì nguy cơ rò rỉ và giả mạo thông tin luôn có thể xảy ra và vượt khỏi tầm kiểm soát của người dùng. Bên cạnh đó, virus máy tính ngày càng lan tràn; vì thế, việc bảo vệ các hệ thống máy tính và dữ liệu khỏi những nguy cơ này là rất cần thiết. Trong phần 1, chúng ta sẽ học một số phương pháp để đảm bảo sự an toàn và bảo mật. Ngoài ra, phần mềm và dữ liệu cần được chuẩn hoá để có thể trao đổi thông tin thông qua mạng. Việc chuẩn hoá có nghĩa là thiết lập các định dạng và cấu trúc chung cho thông tin. Thông tin có thể được trao đổi mà không cần thực hiện thêm bất kỳ thao tác đặc biệt nào nếu như thông tin đã được tập hợp theo đúng với các chuẩn nhất định. Vì vậy trong phần 2, chúng ta sẽ học về các xu thế trong việc chuẩn hoá.

6.1 An toàn bảo mật
6.2 Chuẩn hoá

[Các thuật ngữ và khái niệm cần nắm vững]
Mã hoá, mật mã khóa công khai, mật mã khóa riêng, xác thực, virus máy tính, vắc-

xin, tường lửa, sự giả mạo, sự ngụy trang, ISO9000, MPEG, JPEG, Unicode, EDI, CORBA

6.1 An toàn bảo mật

Mở đầu

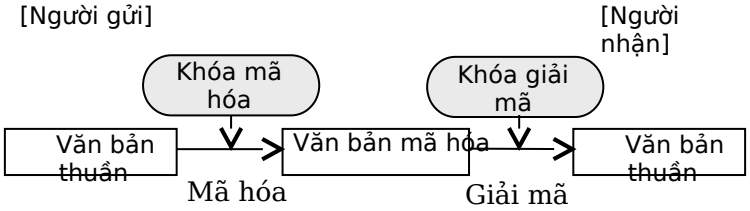
An toàn bảo mật có nghĩa là duy trì tính an toàn của các hệ thống máy tính và các hệ thống mạng. Một cách để ngăn chặn những truy cập trái phép là yêu cầu người dùng nhập vào định danh người dùng (user ID) và mật khẩu của người đó. Một cách khác cũng rất hiệu quả là mã hoá dữ liệu để chống rò rỉ dữ liệu cho bên thứ ba (third party).

6.1.1 Bảo vệ sự an toàn

Điểm chính	➢ **Các phương pháp bảo vệ bao gồm mã hoá, xác thực và quản lí truy cập.** ➢ **Các phương pháp mã hoá bao gồm mật mã khóa riêng và mật mã khóa công khai.**

Mã hoá (Encryption)

Mã hoá có nghĩa là trộn thông tin theo một mẫu nào đó sao cho bên thứ ba không thể hiểu nội dung của nó. Đây là một phương pháp có hiệu quả cao trong việc bảo vệ thông tin lưu trong hệ thống máy tính. Dựa trên sự kết hợp giữa khóa để mã hoá và khóa để giải mã, có hai loại là mật mã khóa riêng (hay còn gọi là mật mã khóa chung) và mật mã khóa công khai. Khái niệm về mã hoá được trình bày dưới đây. [1]



Văn bản thuần: dữ liệu trước mã hóa
Văn bản mã hóa: dữ liệu sau mã hóa

Mật mã	Giải thích
Mật mã khóa riêng	Cùng một khóa được dùng để làm khóa mã hoá và khóa giải mã (chuyển đổi đối xứng). Khóa cần được giữ bí mật. DES và FEAL là những ví dụ về hệ thống này.
Mật mã khóa công khai	Khóa mã hoá là khóa được công khai trong khi khóa giải mã được giữ bí mật. Thông điệp được mã hoá bởi khóa công khai của bên nhận và được giải mã bởi khóa riêng của bên nhận (chuyển đổi bất đối xứng). RSA là một ví dụ cho hệ thống này.[2] [3]

[1] (Gợi ý) Mã hóa không thể ngăn ngừa dữ liệu khỏi bị sai lệch vì nó chỉ làm cho dữ liệu không thể đọc được. Ngoài ra, có một rủi ro là mẫu mã hoá có thể bị bẻ gẫy nếu như cùng một khóa đó được sử dụng trong một thời gian dài. Cần phải biết rằng mã hoá không phải là một biện pháp hoàn hảo.
[2] (Chú ý) Cần biết rằng trong mật mã khóa công khai, mã hoá được thực hiện bằng cách sử dụng

Xác thực

Xác thực có nghĩa là kiểm tra xem người dùng có phải là một người dùng hợp lệ hay không. Có nhiều phương pháp xác thực được liệt kê dưới bảng sau:

Phương pháp	Giải thích
Xác thực thực thể	Là công nghệ xác định tổ chức mà chúng ta đang giao tiếp có hợp lệ hay không. Thông thường người ta sử dụng sự kết hợp giữa ID người dùng và mật khẩu. Ngoài ra còn rất nhiều các phương pháp khác bao gồm call-back, [4] mật mã khoá riêng, và mật mã khoá công khai.
Xác thực thông điệp	Là công nghệ phát hiện bất kì sự sai lệch nào có thể xảy ra trong khi truyền kí tự hoặc văn bản. Nếu như có sự sai lệch, bit kiểm tra sẽ được thiết lập.
Chữ kí số[5]	Là công nghệ đảm bảo sự hợp lệ của một tài liệu, thông thường sử dụng mật mã khóa công khai.

Đôi khi, mật khẩu sử dụng một lần (ngắn hạn) được sử dụng để tăng cường sự an toàn và bảo mật. ID người dùng cũng là một biện pháp để xác thực; thông thường, người quản trị hệ thống chịu trách nhiệm ấn định ID người dùng còn mật khẩu được quản lý bởi người dùng.

Quản lý truy cập

Quản lý truy cập có nghĩa là ngăn cản những truy cập trái phép tới nguồn tài nguyên (ví dụ như dữ liệu) trong một hệ thống máy tính.

Để thực hiện mục đích này, các ID người dùng và mật khẩu đã được đăng kí trước với hệ thống, người dùng được yêu cầu phải nhập ID và mật khẩu của người đó để có được quiền truy cập tới các nguồn tài nguyên và mạng. Quiền có được khả năng truy cập vào nguồn tài nguyên được gọi là quiền truy cập.

---

khóa công khai của bên nhận. Khóa công khai sẵn có trên mạng và ai cũng có thể có còn khóa giải mã được giữ bí mật. Hệ thống này có đặc điểm là việc chuyển đổi đối xứng gần như không thể và việc giải mã cũng là không thể nếu sử dụng khóa mã hoá.

[3] **DES/RSA**: DES (Data Encryption Standard) là ví dụ về mật mã khóa riêng. Còn RSA (Rivest-Shamir-Adleman) là ví dụ về mật mã khóa công khai. RSA được đặt tên theo các chữ cái đầu tiên của tên của ba người đã phát minh ra loại mật mã này.

[4] **Call-back**: Đây là một phương pháp mà bên nhận ngắt kết nối trao đổi và sau đó kết nối lại bằng cách gọi bên gửi trở lại.

[5] **Chữ kí điện tử**: Đây là phương pháp mà áp dụng mật mã khoá công khai. Có rất nhiều cách để ứng dụng phương pháp này, nhưng cách đơn giản nhất là sử dụng mật mã khoá công khai nghịch đảo.
Bên gửi mã hoá văn bản với khoá riêng bí mật của anh ta/cô ta và thêm tên của anh ta/cô ta vào trong văn bản thuần. Bên nhận, dựa vào tên thuần đó, sẽ lấy được khoá công khai của bên gửi và sử dụng khoá công khai đó để giải mã văn bản. Nếu thông điệp đã được mã hoá đó mà đọc được, bên gửi sẽ tiến hành kiểm tra lại; mặt khác, bên nhận sẽ xác định xem thông điệp này có phải là đã được gửi bởi người khác giả mạo hay không.

Bảng sau chỉ ra các phương pháp quản lý truy cập để nhận dạng từng cá nhân.

Kiểu	Giải thích
Tri thức cá nhân	Mật khẩu …
Sở hữu cá nhân	thẻ ID, thẻ IC, thẻ quang …
Đặc điểm cá nhân	Dấu vân tay, giọng nói, hình dạng bàn tay, mẫu võng mạc, chữ kí …

Quản lý quiền truy cập thông qua các đặc điểm cá nhân được gọi là xác thực sinh trắc học.

6.1.2 Virus máy tính

Điểm chính	➢ **Virus máy tính là các chương trình thực thi các hành động không hợp lệ.** ➢ **Tường lửa bảo vệ việc truy cập không được phép từ bên ngoài.**

Cùng với sự phát triển và ngày càng phổ biến của Internet, sự xuất hiện của ngày càng nhiều các kiểu hình thức phá hoại thông qua mạng đang dần trở thành một xu thế. Vì vậy, vấn đề ngày càng trở nên cấp thiết là cần phải có biện pháp ngăn chặn các virus máy tính và bảo vệ ngăn chặn lại những truy cập không được phép từ bên ngoài. Chúng ta sẽ cùng giải thích về vấn đề này một cách chi tiết hơn, bao gồm các phương pháp cụ thể để có thể áp dụng.

Virus máy tính

Một **virus máy tính**, hay chỉ đơn giản, một con **virus**, là một chương trình xâm nhập vào hệ thống thông qua mạng hoặc các thiết bị lưu trữ với mục đích để phá hoại, gây lỗi, hoặc đánh cắp dữ liệu. Một virus máy tính có thể tự tái sinh và sinh sôi thông qua môi trường mạng và các thiết bị lưu trữ. Hơn nữa, bất kì ai cũng có thể tạo ra một virus macro[6] rất dễ dàng, vì vậy thiệt hại do virus gây ra càng lan rộng.

Thông thường, virus máy tính bao gồm ít nhất một trong những chức năng sau:

Chức năng	Đặc tính
Chức năng tự lây	Virus gây ảnh hưởng bằng cách tự tái sinh bằng chính chức năng của nó hoặc tái sinh trên một hệ thống khác sử dụng chức năng của hệ thống.
Chức năng ẩn	Virus bao hàm một số điều kiện xác định để tấn công, ví dụ như ngày giờ, khoảng thời gian, hoặc số lượng tiến trình cụ thể; khi đó virus tự ẩn giấu cho đến khi tiến hành tấn công.
Chức năng thể hiện hội chứng	Virus có một số chức năng để phá huỷ các tệp tin như các chương trình, dữ liệu hoặc thực thi một số thao tác mà người tạo ra không mong đợi.

Vắc-xin (Phần mềm vắc-xin, vắc-xin máy tính)

Vắc-xin là một chương trình có thể tìm ra và loại trừ các virus máy tính. Về cơ bản, vắc-xin chứa một cơ sở dữ liệu có sẵn (một tệp mẫu) mà trong đó đã đăng kí các mẫu về các virus máy tính đã được phát hiện, thực hiện

[6] **Virus macro**: Đây là một loại virus máy tính lợi dụng các hàm macro của các bảng tính và phần mềm xử lí văn bản. Các virus máy tính thông thường đòi hỏi một kiến thức nhất định về ngôn ngữ máy, vì vậy việc tạo ra chúng đối với người dùng là khá khó khăn. Mặc dù vậy, các virus macro có thể được viết bằng các ngôn ngữ lập trình, do đó chúng có thể được tạo ra một cách khá dễ dàng. Thông thường chúng ẩn trong các tệp tin và được gửi kèm cùng với email.

so sánh nhiều loại dữ liệu trên đĩa và bộ nhớ với các mẫu này, từ đó phát hiện ra các virus máy tính. Vì lí do này, việc cập nhật các vắc-xin vào bất kì lúc nào cũng là cần thiết.[7] [8]

[7] (FAQ) Trong các kì thi trước, đã có rất nhiều các câu hỏi liên quan đến virus máy tính. Bạn cần nắm chắc định nghĩa về virus máy tính, các phương pháp để tránh ảnh hưởng của virus, các phương pháp để áp dụng trong trường hợp bị ảnh hưởng, và các vấn đề liên quan đến vắc-xin.
[8] (Gợi ý) Vắc-xin chỉ có thể nhận ra các mẫu của những virus đã từng được phát hiện. Do đó nó không thể xử lí được các virus mới. Vì vậy một gợi ý cơ bản là cần có sự phòng ngừa và thận trọng để sao cho máy tính không bị ảnh hưởng bởi virus. Một khi đã phát hiện ra ảnh hưởng của virus thì cần thiết phải ngay lập tức áp dụng các thao tác để ngăn không cho ảnh hưởng lan rộng hơn.

Các biện pháp ngăn chặn virus

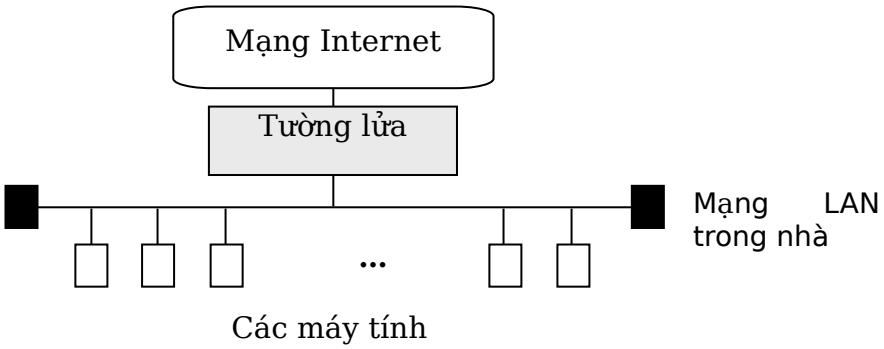
Để bảo vệ máy tính khỏi bị ảnh hưởng bởi các virus máy tính, những điểm sau đây cần được chú ý:

- Có phần mềm vắc –xin
- Không sao chép phần mềm bất hợp pháp
- Không thực thi các chương trình khả nghi
- Thiết lập mật khẩu và quiền truy cập
- Thực hiện sao lưu định kỳ
- Không chia sẻ đĩa cứng (cần chọn lọc trong quản lí)
- Không mở những thư điện tử khả nghi

Nếu chúng ta phát hiện ra ảnh hưởng của virus, cần liên hệ ngay với người quản trị để xin chỉ dẫn. Những hành động tự ý có thể khiến cho tác hại của các virus máy tính càng trở nên trầm trọng.

Tường lửa

Tường lửa là một hệ thống (cơ cấu) bảo vệ hệ thống mạng nội bộ như hệ thống mạng LAN trong nhà, khỏi truy cập trái phép từ bên ngoài. Cụ thể hơn, tường lửa được cài đặt giữa một mạng nội bộ và mạng bên ngoài ví dụ như Internet. Tất cả các giao tiếp giữa bên trong và bên ngoài được thực hiện thông qua tường lửa. Tường lửa có khả năng giới hạn các dịch vụ có sẵn cho mỗi người dùng và xác định quiền truy cập từ bên ngoài để quiết định xem có cho phép truy cập tới mạng bên trong hay không. Đôi khi một máy tính được cài đặt tường lửa, cũng được trang bị chức năng của một máy chủ đại diện[9] (proxy server).



[9] **Máy chủ đại diện**: Đây là một loại máy chủ được cài đặt để bảo vệ tính an toàn bảo mật và truy cập tốc độ cao khi một mạng bên trong kết nối với Internet. Máy chủ này ngăn chặn những sự xâm nhập trái phép vào mạng bên trong và gây trễ, quản lí truy cập từ mạng bên trong ra ngoài Internet. Chức năng này khá giống với chức năng của một tường lửa, và vì vậy thông thường chức năng của máy chủ đại diện được thực hiện bởi một thiết bị tường lửa. Ngoài ra, một máy chủ đại diện còn có chức năng "uỷ nhiệm": dữ liệu gửi đến từ Internet có thể được lưu lại ở đó một cách tạm thời. Sau đó, khi chính trang web đó được truy cập lại, sự truy cập sẽ trở nên nhanh hơn bằng cách bật nó ở máy chủ đại diện.

1.1.1 6.1.3 Tội phạm máy tính

Điểm chính	➢ **Tội phạm máy tính là hành động xâm nhập vào hệ thống thông tin với mục đích không tốt.** ➢ **Virus máy tính là một loại tội phạm máy tính**

Tội phạm máy tính là hành động xâm nhập vào một hệ thống thông tin với mục đích không tốt và thực hiện một hành động nào đó chẳng hạn như phá huỷ dữ liệu. Cùng với sự mở rộng của các hệ thống mạng, những người dùng không có quiền nhưng có thể truy cập vào các mạng đã bắt đầu xuất hiện. Virus máy tính là một phương tiện phổ biến của tội phạm máy tính.
Tội phạm máy tính bao gồm việc thao tác trên mạng của các hệ thống ngân hàng, xâm nhập vào trong một máy tính được điều khiển từ xa thông qua mạng, và đặt bẫy trên các phần mềm tên miền công cộng.

Giả mạo (Falsification)

Giả mạo đề cập đến hành động cố tình làm thay đổi dữ liệu hoặc chương trình trong một máy tính và bao gồm giả mạo hoặc chỉnh sửa tài liệu, thay thế phương tiện lưu trữ bằng một phiên bản lỗi đã được chuẩn bị từ trước, ghi lại dữ liệu và xoá dữ liệu. Việc ngăn chặn giả mạo là rất khó khăn nhưng một phương pháp hiệu quả để phát hiện ra giả mạo là xác thực thông điệp. Một ví dụ cho việc giả mạo là phương pháp Salami.

Phương pháp salami là một cách để đánh cắp dần dần từ một nguồn tài nguyên có số lượng lớn. Ví dụ như, một người dùng có thể mở một tài khoản ngân hàng ảo và chuyển một vài xu từ các tài khoản khác tới tài khoản của anh ta/cô ta.

Sự phá hoại (Destruction)

Sự phá hoại là hành động xoá các dữ liệu quan trọng hoặc một chương trình được lưu trữ trong máy tính và vô hiệu hoá các thiết bị hệ thống hoặc các phương tiện lưu trữ bằng cách phá huỷ chúng một cách vật lý. Những ví dụ điển hình cho hình thức phá hoại này là Trojan horse, bom logic[10] và bom thư điện tử[11].
Một phần mềm **trojan horse** giấu bên trong chương trình một lệnh đặc biệt để không gây ảnh hưởng tới quá trình xử lý thông thường và sau đó thực thi các chức năng không được phép trong khi vẫn để chương trình hoạt động bình thường. Một khi thoả mãn một điều kiện nhất định nào đó, nó có thể phá huỷ tất cả các tệp tin trong máy tính hoặc đánh cắp ID người dùng và mật khẩu. Để ngăn chặn lại Trojan horse, người dùng cần phải cẩn

[10] **Bom logic**: Đây là một chương trình ứng dụng của phương pháp được sử dụng bởi Trojan horse. Chương trình này nhúng bên trong hệ thống một tiến trình gây phá huỷ hệ thống khi thoả mãn một điều kiện nào đó (thời gian, tình huống, tần suất ...)
[11] **Bom thư điện tử**: Đây là hành động gửi một lượng lớn các thư điện tử hoặc thư điện tử có kích thước lớn tới một người xác định trong một khoảng thời gian ngắn, dẫn đến gây lỗi cho hệ thống thư điện tử.

thận lưu lại một bản sao như là bản sao gốc và so sánh chương trình khả nghi với với bản sao đó để phát hiện ra virus. Mặc dù vậy, không có một phương pháp nào thực sự hiệu quả để phòng ngăn chặn Trojan horse bên cạnh việc kiểm tra chương trình nguồn vào thời điểm chương trình đó được ghi hoặc chỉnh sửa.[12] [13]

[12] (FAQ) Trong các kì thi trước, đã có xuất hiện các câu hỏi liên quan đến tội phạm máy tính, bao gồm các vấn đề về virus máy tính... Cần hiểu rõ về trojan horse và scavenging.

[13] (Chú ý) Một loại tội phạm máy tính khác là superzapping. Đây là hình thức lạm dụng chức năng đặc biệt của hệ thống dùng cho tình trạng khẩn cấp (ví dụ như, một chương trình ứng dụng truy xuất tới tất cả các tệp tin và qua đó có thể thay đổi nội dung của các tệp tin đó)

Rò rỉ (Leak)

Rò rỉ là một thuật ngữ chung để cập đến việc đánh cắp thông tin hoặc bản sao từ một hệ thống thông tin. Các phương pháp bao gồm đặt phương tiện truyền trên một đơn vị đầu ra, trộn lẫn các dữ liệu bí mật vào báo cáo đầu ra và làm cho các dữ liệu nội bộ này có dạng như một thông tin khác bằng cách mã hoá nó. Một ví dụ của việc rò rỉ là scavenging (lùng rác).

Scavenging là hành động đánh cắp thông tin khỏi máy tính sau khi một hành động được thực thi. Một người có thể đánh cắp thông tin từ văn bản bị bỏ đi (giống như rác) hoặc thông tin còn lại trên đĩa cứng hay trong bộ nhớ. Một phương pháp hiệu quả để ngăn chặn lại scavenging là xoá tất cả các thông tin trong bộ nhớ được sử dụng để lưu trữ tạm thời và trên đĩa cứng sau khi hoàn thành công việc. [14]

Tapping

Tapping là hành động chặn các dữ liệu trên mạng một cách phi pháp và đánh cắp thông tin hoặc truy cập vào hệ thống máy tính một cách trái phép. Đối tượng của tapping không chỉ gồm dữ liệu máy tính mà còn các dữ liệu âm thanh. Mã hoá là biện pháp hiệu quả để ngăn chặn tapping.

Mạo danh (Disguise)

Disguise is the act of stealing someone else's user ID and password and acting on a network using the stolen identity. By doing so, the unauthorized user steals confidential information that only the authorized user should access, or commits wrongdoing and blames the authorized user for what he or she has done. Digital signatures are effective in preventing disguise.
Mạo danh là hành động đánh cắp ID người dùng và mật khẩu của người khác và hoạt động trên mạng sử dụng các thông tin đánh cắp ấy. Bằng cách làm như vậy, người dùng trái phép có thể ăn cắp các thông tin nội bộ mà chỉ những người dùng hợp pháp có thể truy cập, hoặc có thể thực hiện các hành động trái phép và đổ tội cho người dùng hợp pháp vì những hành động đó. Chữ kí điện tử rất hiệu quả trong việc ngăn chặn lại giả mạo.

[14] (Chú ý) Rất nhiều phương pháp khác nhau được sử dụng để duy trì tính an toàn và bảo mật trong giao tiếp, bao gồm "nhận diện số gọi" và "nhóm người dùng đóng". "Nhận diện số gọi" là cách để thông báo cho người nhận cuộc gọi về số điện thoại của người gọi. "Nhóm người dùng đóng" để đăng kí địa chỉ của thiết bị đầu cuối cho phép tạo kết nối với các đơn vị chuyển đổi điện tử và tạo kết nối chỉ với những thiết bị đầu cuối đó.

Câu hỏi nhanh

Q1 Điền từ thích hợp vào ô trống trong bảng sau

	Khoá mã hoá	Khoá giải mã
Mật mã khoá riêng		
Mật mã khoá công khai		

Q2 Thông thường, một virus máy tính được định nghĩa là có ít nhất một trong ba chức năng. Liệt kê ba chức năng đó.

A1

	Khoá mã hoá	Khoá giải mã
Mật mã khoá riêng	Khoá riêng (khoá chung)	Khoá riêng (khoá chung)
Mật mã khoá công khai	Khoá công khai của bên nhận	Khoá riêng của bên nhận

A2 Chức năng tự lây lan, chức năng ủ bệnh và chức năng thể hiện triệu chứng

6.2 Chuẩn hoá

Mở đầu

Chuẩn hoá có nghĩa là định ra các qui định, yêu cầu, đặc tả, cấu trúc, hoặc/và các định dạng chung. Các đối tượng đã được chuẩn hoá có thể sử dụng mà không cần phải điều chỉnh gì thêm. Những đối tượng chuẩn ở đây liên quan đến xử lí thông tin bao gồm phần cứng, phần mềm, các qui trình để phát triển hệ thống và những qui ước lập trình.

1.1Các tổ chức chuẩn hóa và chuẩn hoá quá trình phát triển và môi trường

Điểm chính	➢ **Các tổ chức chuẩn hóa bao gồm ISO, ITU, ANSI ...** ➢ **Các chuẩn bao gồm ISO 9000, ISO 14000, ...**

Chuẩn hoá cho công nghệ thông tin được thực hiện chủ yếu bởi ISO. Sự chuẩn hoá trong viễn thông được thực hiện bởi ITU. Các tổ chức khác bao gồm ANSI, đây là tổ chức đã đề ra các chuẩn nội địa của Mĩ. Các chuẩn cụ thể bao gồm ISO 9000 cho phát triển phần mềm và chuẩn ISO 14000 cho môi trường. [15]

Các tổ chức chuẩn hoá

Bảng sau là tập hợp các tổ chức chuẩn hoá nổi tiếng:[16] [17]

Tên	Giải thích
ISO	Tổ chức chuẩn quốc tế Đây là tổ chức quốc tế hoạt động để thống nhất và qui định các chuẩn trong các lĩnh vực liên quan đến công nghiệp. Trong mỗi lĩnh vực, thông thường có Ủy ban kỹ thuật (TC) và dưới uỷ ban kỹ thuật là các tiểu ban (SC) và các nhóm làm việc (WG).

[15] (Gợi ý) Trong số các hoạt động về việc chuẩn hoá của tổ chức ISO, hoạt động trong ngành điện tử và điện đã được phần nào hoàn thành cùng với IEC. Làm việc trong viễn thông được phần nào hoàn thành bởi ITU. Đôi khi ISO có thể kết hợp với các tổ chức chuẩn hoá địa phương như là ANSI nếu cần thiết

[16] **IEC(International Electrotechnical Commission - Hội đồng công nghệ điện điện tử quốc tế)**: đây là một tổ chức được thành lập với mục đích định ra các chuẩn quốc tế chung trong lĩnh vực điện điện tử. Tổ chức này hiện nay đã trở thành bộ phận viễn thông của ISO (ISO/IEC), làm việc cùng nhau như một tổ chức.

[17] **IEEE(Institute of Electrical and Electronics Engineers):** Nhóm này có một ảnh hưởng lớn trong việc đề ra các chuẩn trong nhiều lĩnh vực như LAN và các giao thức khác

Tên	Giải thích
ITU	Liên đoàn truyền thông quốc tế Đây là tổ chức quốc tế chuẩn hoá các công nghệ viễn thông cũng như chuẩn hóa và đề xuất các chuẩn quốc tế cho tất cả các loại truyền thông. ITU-T[18] chịu trách nhiệm đối với viễn thông trong khi ITU-R[19] chịu trách nhiệm với các hệ thống không dây và vô tuyến.
ANSI	Viện chuẩn hoá quốc gia Mỹ Đây là một tổ chức phi lợi nhuận tham gia trong việc lập ra các chuẩn công nghiệp ở Mỹ và các nước thành viên của ISO.

Loạt chuẩn ISO 9000

Loạt chuẩn ISO 9000 là tên chung cho một loạt các chuẩn quốc tế được thiết lập bởi tổ chức ISO quan tâm đến cấu trúc đảm bảo chất lượng của các doanh nghiệp. Loạt chuẩn này được thiết lập vào năm 1987, chỉnh sửa vào năm 1994 và chỉnh sửa thêm vào năm 2000 để hình thành ra phiên bản hiện nay. Chuẩn cho việc xác thực là chuẩn ISO 9001; các chuẩn khác chỉ ra các điều khoản được coi như là hướng dẫn để đạt được tính xác thực.

Chuẩn ISO 9001 qui định những yêu cầu có liên quan đến hệ thống quản lý chất lượng cho các doanh nghiệp và tổ chức trong các trường hợp sau:

- Khi cần thiết, phải kiểm tra rằng công ty có khả năng cung cấp sản phẩm thoả mãn những yêu cầu của khác hàng hoặc những chuẩn được yêu cầu thích hợp hay không.
- Khi công ty muốn có được sự hài lòng của khách hàng

Vì vậy, đây được coi là chuẩn cho hệ thống quản lý chất lượng, chứ không phải là chuẩn cho sản phẩm. Từ khi ISO 9001 được công nhận toàn cầu, các công ty đạt được chuẩn này cũng có được sự tín nhiệm của quốc tế.

Cấu trúc của loạt chuẩn ISO 9000 được trình bày từng phần như dưới đây:

ISO 9000		Hệ thống quản lý chất lượng – Cơ bản và từ vựng
	ISO 9001	Hệ thống quản lý chất lượng – Các yêu cầu Trách nhiệm trong việc quản lý (hướng đến khách hàng, các chính sách chất lượng, kiểm điểm,…) Quản lý tài nguyên (Sự phân chia nguồn lực, nguồn nhân lực, môi trường làm việc,…) Hiện thực hoá sản phẩm (kế hoạch hiện thực hoá sản phẩm, các quá trình có liên quan đến khách hàng, thiết kế và phát triển,…) Đo lường, phân tích và cải tiến (điểu khiển và đo lường, điều chỉnh các sản phẩm không phù hợp,…)
	ISO	Hướng dẫn cho các cải tiến về hiệu năng

[18] **ITU-T (International Telecommunications Union – Telecommunications Standardization Sector)**: Đây là bộ phận thảo luận về công nghệ, giao tiếp và các phí có liên quan đến điện thoại và điện báo; bộ phận này cũng đưa ra các chuẩn riêng của họ như là những đề xuất. Những đề xuất chính của bộ phận này bao gồm loạt I cho ISDN, loạt V cho các đường dây tương tự và loạt X cho các đường dây kĩ thuật số.

[19] **ITU-R (International Telecommunications Union – Radiocommunication Sector)**: Đây là bộ phận được giao cho các tần số của sóng radio, các hệ thống radio chuẩn, các thao tác giao tiếp vệ tinh, giao tiếp thông qua không dây, giao tiếp di động, phát thanh truyền hình,…

	9004	

Loạt chuẩn ISO 14000

Loạt chuẩn ISO 14000 là một nhóm các chuẩn quốc tế được lập ra bởi tổ chức ISO liên quan đến quản lý bảo vệ môi trường. Các chuẩn này đặt ra các hướng dẫn cho việc đo lường mà các công ty phải thực hiện để xử lý các vấn đề ảnh hưởng xấu tới môi trường toàn cầu như là sự tiêu thụ nguồn năng lượng và rác thải công nghiệp. Các chuẩn này tương đương với phiên bản về môi trường của loạt chuẩn ISO 9000 và hệ thống hoá các chứng chỉ tuân theo bởi một tổ chức thứ ba. [20]

[20] (FAQ) Một số câu hỏi thi hỏi về vai trò của các tổ chức chuẩn quốc tế bao gồm ISO và ITU. Mặc dù vậy, hầu hết các câu hỏi thi đều giả thiết là bạn đã có những hiểu biết trước đó về các chuẩn này. Một ví dụ tiêu biểu cho những câu hỏi như vậy là "Định dạng nén ảnh nào được chuẩn hóa bởi cả hai tổ chức ISO và IEC". Cần chắc rằng bạn biết ít nhất là tên gọi và vai trò của các tổ chức đề ra chuẩn đã được đề cập đến trong quiển sách này.

6.2.2 Chuẩn hoá dữ liệu

Điểm chính	➢ **Các mã kí tự bao gồm EBCDIC, Unicode ...** ➢ **Các định dạng tệp tin bao gồm JPEG, MPEG, SGML, CSV, ...**

Khi truyền dữ liệu, một trong những quá trình sau đây cần phải thực hiện: gửi dữ liệu sau khi làm cho dữ liệu tương thích với định dạng của bên nhận; hoặc nhận dữ liệu dưới một định dạng khác và sau đó chuyển nó về định dạng dữ liệu của bên nhận. Trong cả hai cách, nếu như định dạng không nhất quán, cần phải chuyển chúng cho những tổ chức khác. Mặc dù vậy, việc thay đổi định dạng có thể được loại trừ nếu như có những định dạng chuẩn và tất cả mọi người đều sử dụng định dạng chuẩn này. Dữ liệu được chuẩn hoá ở đây bao gồm các mã kí tự và định dạng tệp tin.

Mã kí tự

Mã kí tự là mã được gán cho mỗi kí tự và kí hiệu với mục đích xử lý kí tự và các kí hiệu đó trên máy tính. Các mã kí tự được xử lý khác nhau phụ thuộc vào máy tính xử lý.

Mã	Giải thích
EBCDIC	Mã chuyển đổi nhị phân thập phân mở rộng (Extended Binary Coded Decimal Interchange Code) Đây là mã kí tự được IBM thiết lập dành cho các máy tính với mục đích chung. Một tập hợp gồm 8 bit đại diện cho một kí tự.
Unicode (UCS-2)	Chuẩn để biểu diễn một kí tự được sử dụng trên toàn thế giới chỉ trong một mã kí tự hợp nhất. Tất cả các kí tự được biểu diễn sử dụng 2 byte. Đây được coi là một phần của chuẩn quốc tế được đưa ra bởi ISO.

Bổ sung thêm vào danh sách các mã được liệt kê ở bảng trên, có chuẩn ASCII[21] và EUC[22] và các chuẩn khác.[23]

Tệp tin hình ảnh

Tệp tin hình ảnh là tệp tin mà trong đó một ảnh tĩnh giống như ảnh chụp hoặc ảnh kỹ xảo minh hoạ được số hoá thành một tệp tin. Có rất nhiều định dạng tệp tin được liệt kê dưới đây.

[21] **ASCII** (**American Standard Code for Information Interchange**): Đây là mã kí tự được thiết lập bởi ANSI, tạo nên các mã cho các kí tự chữ cái, số, các kí tự đặc biệt, và các kí tự điều khiển như là dấu xuống dòng, mỗi mã sử dụng 7 bit. ASCII được coi là một phần của chuẩn quốc tế ISO (ISO 646).

[22] **EUC** (**Extended Unix Code**): Đây là mã kí tự bất kì, được sử dụng chủ yếu bởi hệ điều hành UNIX. Nó có thể xử lí các kí tự 2 byte cũng như là các kí tự 1 byte. Đây là mà chuẩn được đề xuất bởi AT&T và EUC Nhật Bản, EUC Hàn Quốc và EUC Trung Quốc,...

[23] (Chú ý) Sau chuẩn đầu tiên, Unicode đã được mở rộng để sử dụng 3 byte hoặc nhiều hơn. Vì vậy, ngày nay nó được định nghĩa để cho mỗi kí tự có thể sử dụng 4 byte trong Unicode (UCS-4).

Định dạng	Giải thích
JPEG	Joint Photographic Experts Group: Một tổ chức kết hợp của ISO và ITU-T nhằm mã hoá màu sắc trong ảnh tĩnh, hoặc phương pháp nén/ giải nén được đề ra bởi tổ chức này.
GIF	Graphic Interchange Format: Định dạng ảnh được phát triển bởi CompuServe, một công ty dịch vụ trực tuyến lớn ở Mỹ. Nó tương thích với các ảnh màu hoặc ảnh đơn sắc với số màu là 256 hoặc ít hơn.
BMP	Format to save images as bitmap data, standard graphics format used by Windows. Định dạng để lưu giữ ảnh dưới dạng dữ liệu từng bit, định dạng đồ hoạ chuẩn được sử dụng bởi hệ điều hành Windows.
TIFF	Target Image File Format: Để biểu diễn dữ liệu sử dụng các thẻ đặt trong khối dữ liệu ở trong tệp tin. Bằng cách sử dụng các thẻ, ta xác định được định dạng của dữ liệu.

Nén ảnh động

Một hệ thống mã cho ảnh động là MPEG (Moving Picture Experts Group). MPEG là tên của tổ chức nhỏ của JTC1, là tổ chức kết hợp giữa ISO và IEC. Đây là phương pháp để nén/giải nén ảnh động, được đề xuất bởi nhóm này.[24]

Định dạng tệp tin văn bản

Tệp tin văn bản được chuẩn hoá với mục đích là các dữ liệu văn bản và dữ liệu được chuẩn bị sử dụng một ứng dụng có thể dễ dàng được chuyển đổi. Một cách qui ước, các tệp tin văn bản được chuyển đổi dưới định dạng được gọi là tệp tin văn bản (*.txt). Mặc dù vậy, các tệp tin văn bản chỉ có thể biểu diễn các xâu kí tự, không thể biểu diễn các đinh dạng viết đa dạng khác như là độ dày của chữ, kích cỡ, màu sắc, và cấu trúc của văn bản tài liệu. Ngày nay, các định dạng đã được chuẩn hoá bao gồm cả kiểu tài liệu. Bằng cách chuẩn hoá các định dạng tệp tin tài liệu, các tài liệu được xử lý theo cách hợp nhất và còn có thể đưa cả vào trong cơ sở dữ liệu.

Bảng sau chỉ ra các định dạng tệp tin tài liệu chuẩn:

Định dạng	Giải thích
SGML	Standard Generalized Markup Language – Ngôn ngữ đánh dấu tổng quát chuẩn Một loại ngôn ngữ biểu diễn cấu trúc ngữ nghĩa và logic của tài liệu cùng các kí hiệu; một tài liệu có thể được sử dụng như một cơ sở dữ liệu.
XML	eXtensible Markup Language – Ngôn ngữ đánh dấu mở rộng được Một loại ngôn ngữ ra đời sau HTML, mà các chức năng mở rộng của SGML có thể được sử dụng trên Web. Người dùng có thể định nghĩa các thẻ riêng của mình.

[24] (Chú ý) MPEG cũng mã hoá cả âm thanh cùng với ảnh động. MPEG có MPEG-1, MPEG-2, MPEG-3, MPEG-4 và nhiều hơn thế nữa. MPEG-1 dùng cho các phương tiên lưu trữ như CD-ROM và là chuẩn cho ISO/IEC (ISO 9660). MPEG-2 là phiên bản nâng cấp của MPEG-1 và dùng cho HDTV(TV có độ phân giải cao) cũng như là việc truyền tải ảnh sử dụng đường truyền băng thông rộng ISDN. MPEG-4 là mã hóa hiệu năng cao cho ảnh động và âm thanh được thiết kế cho mạng Internet và giao tiếp truyền thông qua sóng vô tuyến (truyền thông di động).

HTML	HyperText Markup Language – Ngôn ngữ đánh dấu siêu văn bản Một loại ngôn ngữ được dùng để tạo ra các trang Web trên mạng Internet. Các thẻ được bao trong cặp “< >” để thiết lập ra kích cỡ chữ, màu sắc, và các siêu liên kết.
TeX	Được phát âm là “tek” hoặc “tef” Một chương trình định dạng và hoàn tất tài liệu để có thể thiết lập và in ra các tài liệu với các công thức toán học, hoá học phức tạp.
CSV[25]	Comma Separated Value Format – Định dạng giá trị được phân cách bởi dấu phảy Mỗi thành phần của dữ liệu được đi kèm bởi một dấu phảy và được liệt kê. Định dạng này được sử dụng chủ yếu để lưu giữ dữ liệu từ cơ sở dữ liệu của phần mềm và các phần mềm bảng tính.
PDF	Portable Document Format – Định dạng văn bản di chuyển được Một loại định dạng được phát triển bởi Adobe System cho các tài liệu điện tử. Các tài liệu có thể được trao đổi cho dù trên bất kì mô hình máy tính và nền tảng nào.

[25]

6.2.3 Chuẩn hóa trao đổi dữ liệu và phần mềm

Điểm chính	➢ **Các chuẩn về trao đổi dữ liệu bao gồm EDI, STEP, CALS,...** ➢ **Các chuẩn về phần mềm bao gồm CORBA, RFC, OMG,...**

Để thực hiện những giao dịch trao đổi dữ liệu giữa các công ty, các dữ liệu trao đổi cần phải được chuẩn hoá. Một trong những khái niệm chuẩn hoá này là **EDI**. [26] Ngoài ra còn có **STEP**, đây là một trong những chuẩn trao đổi dữ liệu mô hình sản phẩm. Nếu như các sản phẩm phần mềm tối ưu có thể được kết hợp cùng nhau, bao gồm các phần mềm được viết bởi nhiều hãng sản xuất phần mềm, ta sẽ có một hệ thống tốt hơn. Để thực hiện điều này, phần mềm cũng phải được chuẩn hoá.

Chuẩn hoá trao đổi dữ liệu

Mạng Internet ngày càng trở nên phổ biến và cùng với sự phát triển đó, một loại định dạng mới cũng được ra đời. Loại định dạng này được ra đời để phục vụ các giao dịch trao đổi thông tin điện tử thông qua mạng. Vì lí do này, việc chuẩn hoá trao đổi dữ liệu cũng được xem xét. Bảng sau chỉ ra những phương pháp chuẩn hoá chính.

Loại chuẩn	Giải thích
EDI	Trao đổi dữ liệu điện tử (các giao dịch điện tử, trao đổi dữ liệu điện tử)
CALS	Commerce At Light Speed Tất cả các thông tin liên quan đến sản phẩm được chia sẻ, từ đặc tả, phát triển, thiết kế đến thu nhận, vận hành, và bảo trì. Chuẩn này được thiết kế để nâng cao hiệu suất, rút ngắn giai đoạn phát triển và giảm giá thành.
EC	Thương mại điện tử Buôn bán không phải diễn ra trong các cửa hàng, đặt hàng qua thư mà diễn ra ở trên mạng Internet. Tiền điện tử [27] được coi là phương tiện để thanh toán điện tử.
STEP	Chuẩn để trao đổi các dữ liệu mô hình sản phẩm (Standard for the Exchange of Product Model Data) chuẩn ISO 10303 International standard for the exchange of product model data Là chuẩn quốc tế phục vụ việc trao đổi các dữ liệu mô hình sản phẩm

[26] (Gợi ý) EDIFACT được áp dụng ở Mỹ và Châu Âu, được dùng giúp việc trao đổi dữ liệu giữa các nước hiệu quả hơn.

[27] **Tiền điện tử:** đây là phương thức thanh toán sử dụng giao tiếp qua IC hoặc PC, có đặc điểm là các hóa đơn thanh toán vật lí và tiền mặt không được sử dụng. Tiền điện tử được sử dụng như phương tiện thanh toán trong thương mại điện tử qua mạng, chẳng hạn như mạng Internet. Ngoài ra, có những thẻ IC, nhỏ như thẻ thương mại, được trang bị các chíp điện tử mà trên đó lưu trữ một lượng tiền nhất định, qua đó người dùng có thể mang đi và sử dụng như tiền mặt bình thường.

Open Systems – Các hệ thống mở

Một hệ thống mở là một hệ thống máy tính được tạo nên theo cách mà, bằng việc chuẩn hoá các đặc tả, phần cứng và phần mềm, có thể thực hiện các chức năng mà không gây nên xung đột đối với tất cả các nhà sản xuất. Trong các hệ thống xử lý phân tán, phần cứng xuất phát từ rất nhiều nhà sản xuất khác nhau và thường được kết nối với nhau để hình thành nên một hệ thống; vì vậy, phần cứng và phần mềm đều phải được chuẩn hoá.

Chuẩn hoá phần mềm

Phục vụ cho việc chuẩn hoá phần mềm hướng đối tượng, dưới đây là các phần mềm, các chuẩn và các tổ chức đề ra chuẩn.

Tên	Giải thích
CORBA	Common Object Request Broker Architecture Là những đặc tả chung để các đối tượng có thể trao đổi thông điệp với nhau trong một môi trường hệ thống phân tán. Được đề ra bởi OMG (Object Management Group).
EJB	Enterprise JavaBeans Là các đặc tả chuẩn cho việc hình thành nên những ứng dụng hướng đối tượng phân tán của Java. Có thể kết hợp các thành phần sử dụng các công cụ từ các nhà cung cấp khác nhau. EJB có khả năng tương thích với CORBA.
RFC	Request for Comments Một nhóm các tài liệu về đề xuất kỹ thuật và chú thích, được biên soạn bởi IETF. Các tài liệu này có sẵn trên mạng Internet và có thể được thu được nhờ FTP hoặc email. Giao thức liên quan đến TCP/IP… được viết bằng RFC.
OMG	Object Management Group Một tổ chức phi lợi nhuận đề xuất ra việc phổ biến và chuẩn hoá công nghệ hướng đối tượng. Tổ chức này đề xuất ra chuẩn công nghiệp (OMA) trong lĩnh vực công nghệ hướng đối tượng.

Câu hỏi nhanh

Q1 Mô tả nội dung của loạt chuẩn ISO 9000

Q2 (1) Định dạng nén cho các ảnh màu tĩnh là gì?
(2) Định dạng nén cho các ảnh động là gì?

A1 Loạt chuẩn ISO 9000 là tập các chuẩn quốc tế cho các cấu trúc đảm bảo chất lượng và những nguyên tắc chứng tỏ khả năng của một công ty hay tổ chức có thể cung cấp các sản phẩm theo yêu cầu của khách hàng. Do loạt chuẩn ISO 9000 được công nhận trên toàn thế giới nên công ty nào có được chuẩn này thì cũng sẽ có được danh tiếng quốc tế về sự đáng tin cậy.

A2 (1) JPEG
(2) MPEG

Câu hỏi 1

Độ khó: * Tần suất: ***

Q1. Qui trình nào sau đây đảm bảo người gửi gửi một tài liệu đã được mã hoá cho người nhận bằng cách sử dụng mật mã khoá công khai?

a) Người gửi mã hoá tài liệu bằng cách sử dụng khoá công khai của riêng mình và bên nhận giải mã tài liệu bằng cách sử dụng khoá riêng của anh ta.
b) Người gửi mã hoá tài liệu sử dụng khoá riêng của anh ta, bên nhận giải mã tài liệu bằng cách sử dụng khoá công khai
c) Người gửi mã hoá tài liệu bằng cách sử dụng khoá công khai của bên nhận, và bên nhận giải mã tài liệu bằng cách sử dụng khoá riêng của anh ta
d) Người gửi mã hoá tài liệu bằng cách sử dụng khoá riêng của bên nhận, và bên nhận giải mã tài liệu bằng cách sử dụng khoá riêng của anh ta

Đáp án câu 1

Đáp án đúng: c

Mật mã khoá công khai là một hệ thống mà trong đó khoá mã hoá được đưa ra công khai trong khi khoá giải mã được giữ bí mật. Khoá được đưa ra gọi là khoá công khai, và khoá được giữ bí mật được gọi là khoá riêng. Không giống như mật mã khoá riêng (mật mã khoá chung), chỉ có một khoá mã hoá và một khoá giải mã là cần thiết, vì vậy việc quản lý các khoá là dễ dàng hơn. Hơn nữa, do khóa giải mã được chia sẻ công khai, khoá này không nhất thiết phải gửi đi. Nhưng do khoá công khai không thể được sử dụng để giải mã văn bản, mã hoá và giải mã có thể gây tốn thời gian.
Trong mật mã khoá công khai, bên gửi mã hoá thông điệp bằng cách sử dụng khoá công khai của bên nhận trong khi bên nhận giải mã thông điệp sử dụng khoá riêng của anh ta/cô ta.

a) Trong mật mã khoá công khai, những gì đã được mã hoá bởi khoá công khai, được giải mã bởi khoá riêng cùng cặp với khoá công khai. Trong lựa chọn (a), khoá công khai thuộc về người gửi trong khi khoá riêng thuộc về bên nhận, do đó chúng không tạo nên một cặp.

b) Câu này mô tả về chữ kí điện tử.

d) Một khoá riêng được giữ bí mật. Câu trả lời nói rằng “người gửi mã hoá tài liệu bằng cách sử dụng khoá riêng của bên nhận ” nhưng người gửi không có khoá riêng của bên nhận.

Câu hỏi 2

Độ khó: ** Tần suất: ***

Q2. Câu nào sau đây mô tả thích hợp về virus máy tính?

a) Ngay cả khi trong máy tính tồn tại một tệp tin chương trình mà virus nằm ẩn trong đó, chừng nào mà người dùng còn chưa cố tình khởi động tệp tin đó, máy tính sẽ không bị ảnh hưởng.
b) Virus phá huỷ bộ nhớ chính một cách vật lý và khởi động các thao tác mà không theo chủ ý của người sử dụng.
c) Một máy tính được cập nhật với các thành phần mới nhất và tệp tin chữ kí mới nhất để phát hiện và kiểm tra virus sẽ không bị ảnh hưởng bởi virus.
d) Trong quá trình kiểm tra virus, người dùng có thể tránh bị ảnh hưởng từ sector khởi động bằng cách sử dụng đĩa khởi động hệ điều hành không có virus.

Đáp án đúng: d

Khi một máy tính được bật, ổ đầu tiên mà hệ thống đọc chương trình được gọi là ổ đĩa khởi động, và đĩa cứng hoặc đĩa mềm được dùng như là ổ đĩa khởi động được gọi là đĩa khởi động. Một đĩa khởi động được chuẩn bị trước để sử dụng trong trường hợp khẩn cấp. Khi vùng khởi động bị ảnh hưởng bởi virus, hệ điều hành sẽ được khởi động từ một đĩa khởi động không có virus.

a) Một virus sector khởi động (gọi đơn giản là virus khởi động) xâm nhập vào sector khởi động mà trong đó chương trình khởi động (chương trình khởi động hệ điều hành từ đĩa cứng) được lưu trữ và tấn công máy tính khi máy được bật. Vì vậy, ảnh hưởng của virus có thể xảy ra ngay cả khi người dùng không nhận thức được.

b) Vì virus là một chương trình nên virus không phá huỷ đến phần cứng mặc dù nó có thể gây phá huỷ phần mềm.

c) Một thành phần (phần mềm) để phát hiện và ngăn chặn lại virus được gọi là vắc-xin (phần mềm vắc-xin, vắc-xin máy tính). Một tệp tin chữ kí lưu trữ thông tin về các virus được phát hiện trước đó. Vắc-xin phát hiện và kiểm tra các virus bằng cách kiểm tra những chương trình mục tiêu và các dữ liệu trong tệp tin chữ kí. Do đó, một vắc-xin không thể phát hiện hoặc loại bỏ những virus mới chưa được đăng kí trong tệp tin chữ kí.

Câu hỏi 3

Độ khó: * Tần suất: ***

Q3. Phát biểu nào dưới đây là mô tả phù hợp với chứng chỉ ISO 9001:2000?

a) Khi đã được chứng nhận, chất lượng đã phần nào được đảm bảo.
b) Chỉ có một hội đồng chứng chỉ cho mỗi quốc gia.
c) Đây là chứng chỉ cho lĩnh vực công nghiệp và không được áp dụng cho lĩnh vực dịch vụ.
d) Chứng chỉ chứng nhận các tổ chức mà hệ thống quản lý chất lượng phù hợp với chuẩn quốc tế.

Đáp án câu 3

Đáp án đúng: d

Loạt chuẩn ISO 9000 là tập các thuật ngữ đề cập đến một loạt các chuẩn quốc tế được đề ra bởi tổ chức ISO liên quan đến hệ thống quản lý chất lượng của các công ty. Chuẩn dùng để chứng nhận là ISO 9001, và các chuẩn khác là các mục chỉ ra các nguyên tắc để đạt được chứng chỉ ISO 9001. Đây không phải là chuẩn cho sản phẩm, hơn thế nữa, nó chứng nhận một cách quốc tế là qui trình chất lượng của công ty hoặc tổ chức là dựa trên những điểm sau:

- Các công ty hoặc tổ chức đó có khả năng để cung cấp các sản phẩm thoả mãn nhu cầu của khách hàng hoặc đáp ứng được các chuẩn theo yêu cầu.
- Họ đang làm việc để nâng cao sự thoả mãn của khách hàng.

Một cách tình cờ, chuẩn ISO 9001 được xem xét lại vào tháng 12 năm 2000. Các mục được yêu cầu trước đây bị phân tán, nay đã được tổ chức lại và chia thành bốn nhóm: “Trách nhiệm quản lý”, “Quản lý tài nguyên”, “Hiện thực hoá sản phẩm”, “Đo lường, phân tích và cải tiến”. Chuẩn này có đặc điểm là khái niệm về hệ thống quản lý chất lượng và sự cải tiến không ngừng của hệ thống quản lý chất lượng. Con số “2000” trong “ISO 9001:2000” biểu thị là chuẩn này được xem xét lại vào năm 2000.

a) Một công ty được chứng nhận cần phải được kiểm tra hàng năm hoặc mỗi sáu tháng, và việc đánh giá lại một cách đầy đủ cần phải được thực hiện mỗi 3 năm. Vì vậy, những hoạt động liên tục là rất cần thiết.
b) Có rất nhiều tổ chức chứng nhận. Một tổ chức mong muốn được chứng nhận có thể chọn bất kỳ tổ chức chứng nhận nào theo ý mình. Mặc dù vậy, mỗi quốc gia chỉ có duy nhất một tổ chức được uỷ nhiệm mà có thể kiểm tra và công nhận các hội đồng chứng nhận khác.
c) Chuẩn này áp dụng cho tất cả các ngành.